

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 February 2002 (21.02.2002)

PCT

(10) International Publication Number
WO 02/15077 A1

(51) International Patent Classification⁷: **G06F 17/60**,
11/30, 12/14, H04L 9/00, 9/32, G11B 3/70, 5/84, G06B
7/26, G06K 5/00, G07F 11/00.

(21) International Application Number: PCT/US00/22373

(22) International Filing Date: 14 August 2000 (14.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **STARPAY.COM, INC.** [US/US]; Suite 320,
5600 N. May Avenue, Oklahoma City, OK 73122 (US).

(72) Inventor: **MESSNER, Marc, A.**; 111 S. Crosstimber
Trail, Edmond, OK 73034 (US).

(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK,

DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL,
IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU,
LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT,
RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA,
UG, UZ, VN, YU, ZA, ZW.

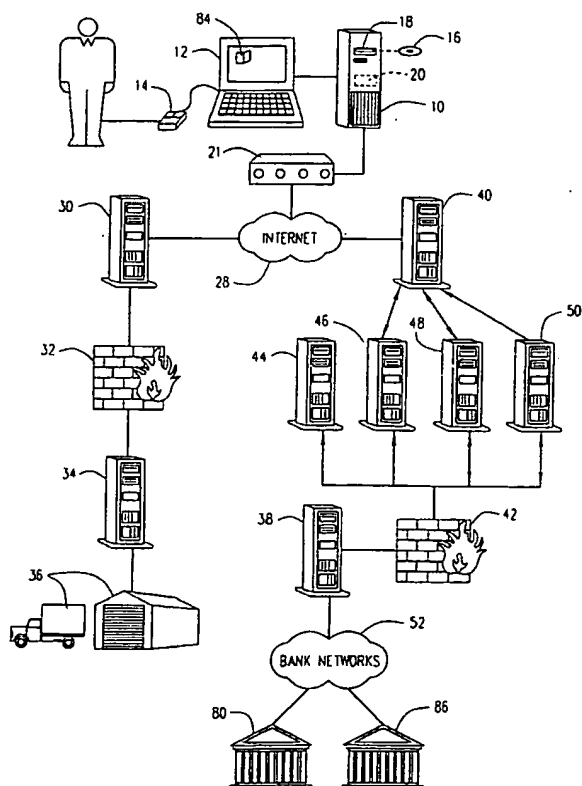
(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian
patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European
patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG,
CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: APPARATUS AND METHOD FOR PERFORMING SECURE NETWORK TRANSACTIONS



(57) Abstract: An apparatus and method for performing secure network transaction (Fig. 1) utilizes a purchasing method (Fig. 3B) and an electronic article (16) and apparatus (10) for providing security for electronic transactions. The electronic article (16) is removably inserted into an electronic apparatus (10), the article (16) bearing machine readable software/codes (22). Proper electronic codes (22) on the article (16), coupled with specific electronically resident codes (20) on the apparatus (10), allow the new purchasing method (Fig. 3B) for electronic transactions (Fig. 1) to securely commence.

WO 02/15077 A1

TITLE OF THE INVENTION

Apparatus and Method for Performing Secure Network Transactions.

5

CROSS REFERENCES TO RELATED APPLICATIONS

None.

BACKGROUND OF THE INVENTION

a. Field of the Invention

10

The invention relates to devices and methods for securing electronic transactions. More particularly, the invention relates to devices and methods designed to protect confidential information and secure transmissions made via electronic networks.

b. Description of the Prior Art

15

The concept of electronic transactions is relatively new. Ignoring transactions pursuant to telephone calls involving a real person on each end, the concept of electronic transactions between two electronic devices was practically unknown until banks pioneered electronic transactions for wire transfers of large quantities of cash.

20

With the rise of the Internet in the early 1980s, long distance electronic transactions became possible for the general public. However, electronic commerce transactions were still relatively rare outside of the above-noted banking transactions until the early 1990s. This was partly because the technologies required for such transactions were not well developed. Also, until the early 1990s there were still a relatively small number of consumers with access to the Internet.

The term "Internet" will be used throughout this document. As used herein, "Internet" means a network of machines accessible to / by multiple users, the machines having the capability, using a common communication protocol, of communicating pursuant to programming commands or information input by users. One specific embodiment of the term
5 Internet is the computer network currently operating to allow users to communicate with remote servers using the common programming language HTML. The terms "computer network," "long distance network," "electronic network" and other variations of these phrases may be used interchangeably in this document, and are intended to be coextensive with the term "Internet."

Recently, there has been an exponential increase in the number of people with access to
10 the Internet. Consequently, Internet business has proliferated. Great quantities of capital have poured into businesses related to the Internet. However, the full potential of the Internet for commercial transactions has not been realized. This is in large part due to concerns among consumers about the security of transactions over the Internet. A 1999 study by Ernst & Young addressed the reasons why consumers had not purchased goods, services or information on the
15 Internet: 97% stated that they were uncomfortable sending credit card data across the Internet. "Internet Shopping Study: The Digital Channel Continues to Gather Steam," page 11, Ernst & Young, LLP (1999) (study sponsored by the National Retail Federation).

Consumers' concerns are justified to some extent. There are at least two types of theft which can occur with Internet transactions: First, communications containing confidential
20 information can be intercepted by parties other than the intended recipient; Second, what appears to be a legitimate business, may actually be a front for con men. Confidential information transmitted over the Internet can be intercepted by hackers. These hackers can then use that confidential information to commit fraud or theft (for example, making charges on credit card information intercepted on the Internet). Also, when a user / customer purchases goods or

services over the Internet, there is little, if any, way for the customer to know that the merchant / supplier is legitimate. A web site which appears to be a legitimate business may, in fact, be a front established by con artists who plan to use the credit card and other information they obtain to defraud unsuspecting consumers.

5 In order to reduce security concerns, there are currently two primary competing technologies vying for dominance to provide "secure" Internet transactions: (1) Secure Sockets Layer ("SSL") protocol and (2) Secure Electronic Transactions ("SET"). Both of these technologies assume that transactions on the Internet will use existing means of payment, most commonly credit card accounts (such as Visa®, Mastercard®, American Express®, and the like).
10 SSL and SET are basically mathematical tools designed to encrypt the data related to these existing means of payment, to minimize the risk that this data may be intercepted and misused by an unintended recipient. Both SSL and SET also incorporate communication paths intended to ensure the integrity of transmissions. SET goes further than SSL in verifying the authenticity of entities using the system. Each user in SET is assigned unique identifiers and are given keys
15 tied to their identifier. For purposes of this document, technology such as SSL and SET may be referred to as "encryption methods," which is also intended to include other methods of encrypting data.

 A November 2, 1998, White Paper by the Gartner Group was titled "SET Comparative Performance Analysis" ("White Paper"). The White Paper compared the performance of SET
20 to the performance of SSL on existing computing technology. The White Paper also speculated about what improvements in technology, anticipated to occur in the near future, will mean to the performance of both SET and SSL. The White Paper addressed criticism of SET, which alleged that its performance was slow which would result in either an unacceptable customer experience or an unjustified investment to ensure sufficient speed for the customer. The White Paper

concluded that SET, which is more secure than SSL, is in fact slower. Hardware acceleration will be required for current technologies to use SET. The White Paper anticipated that as servers improve in performance such acceleration will not be necessary. However, for large e-commerce server applications, the support of SET requires an additional hardware acceleration in the medium term resulting in a five to six percent difference in server costs. Thus, though SET provides greater security, it also provides greater burdens.

SSL "Secure Sockets Layer" protocol is in common use today in many e-commerce servers. SSL offers "session-level" security. This means that once a secure session is established, all communication over the Internet is encrypted. Effectively, using SSL is the equivalent of using a scrambler on the telephone line over which a customer is placing a catalogue purchase using traditional telephones. Data sent from the customer arrives at the merchant's website, the information is decrypted then used by the merchant. How the information is stored and used by the merchant is completely out of the control of the user. Under SSL the customer: (1) has to trust the merchant will guard their credit card information securely, and the customer is assuming a risk in doing so; and (2) the customer has no assurance that the merchant is authorized to accept credit card payment.

By contrast SET insures that both the merchant and the customer are who they appear to be. That is, it insures that the merchant is actually a provider of goods and services who is authorized to receive and process credit card transactions. Similarly, SET insures that the customer is in fact the person who is authorized to use the credit card number being supplied. Whereas with SSL, all information sent on a secure connection is encrypted, with SET, only sensitive information (for example name, address, credit card number, etc.) is encrypted. Thus, the non-encrypted information sent using the SET protocol is faster than SSL. However, the overall performance of SET is slower than SSL.

The Nextcard® has attempted to address the issues of security and customer confidence in a different way. The Nextcard is called a "VISA card for Internet users." The Nextcard attempts to safeguard a user / consumer's credit information by physically storing the information in an extremely secure environment. In addition, SSL is used for all transactions involving the Nextcard. The basic premise, however, of Nextcard is that "when you use your Nextcard VISA to make purchases over the Internet, you are never liable for fraud." Nextcard guarantees customers that they will not incur losses due to fraud over the Internet. There are no restrictions regarding the sites from which a Nextcard customer can make purchases. Similarly, if the Nextcard® is stolen by a merchant, the customer is not liable. If the real card is stolen by someone who then attempts to use the card on the Internet, a customer is still protected. A customer using a Nextcard online, should have no worries about security or the like. He is substantially protected by the "safe shopping pledgeSM."

However, all of the above systems suffer from the same flaw regarding the Internet: namely, they attempt to adapt a set up which was designed for purchases made at a merchant's facility to the needs of the Internet. The basic system used for VISA, Mastercard and other cards was not designed with commerce on the Internet in mind. Therefore, traditional VISA and Mastercard systems adapted to use online cannot take full advantage of the computer environment provided by the Internet.

20

SUMMARY OF THE INVENTION

In view of the foregoing disadvantages inherent in the known types of means for securing electronic transactions, it is an object of the invention to provide an apparatus and method which overcomes the various disadvantages of the prior art.

It is therefore an object of the invention to provide a means for facilitating online transactions, and for insuring the security of such transactions. It is an object of the present invention to provide a system to take the place of traditional Visa, Mastercard or other credit card systems for executing purchases online.

5 It is a further object of the invention to provide a credit card-like system which is available for use exclusively on the Internet. It is also an object of the invention to provide features for the Internet-only credit card system which take full advantage of the computer environment. For example, it is an object of the present invention to provide a billing system used in conjunction with the Internet only credit card whereby billing statements, instead of
10 being sent by regular mail, are sent by e-mail to the customer. This takes advantage of the fact that e-mail is free, incurring no mailing charges for the credit card issuer. In addition, billing transactions are more rapidly completed as are payment transactions. In fact, using the present invention, there could be transactions that are completely paperless. That is, transactions where no paper is sent from or to any of the parties involved in the transaction.

15 It is a further object of the present invention to incorporate features of electronic "wallets" which lessen the burden on a user executing an Internet transaction. In essence, using the present invention and a "wallet," the only data required to be entered by a user to execute a transaction would be a pin number and the description of goods or services to be purchased. In addition, where a user has more than one account of the type employing the present invention, the wallet
20 will allow a user to select the proper account he wishes to use for a transaction.

It is a further object of the present invention to provide a secure system for purchases online. The security of the system is insured by the requirement that a user desiring to execute purchases online must have a digital information storage device (referred to herein as an article or media) physically present in his computer system. If the article is not present, the transaction

cannot be completed. This "article" takes the place of a traditional credit card in real world purchasing systems. That is, the "article" is a physical asset, under the control of the user, which, if not present, invalidates or disables the purchasing system. Thus, a thief, acquiring a card number from this system would not be able to execute purchases without having the physical asset present also. This substantially complicates a thief's job in attempting to use a credit card number without the owner's authorization.

It is also an object of the present invention to provide an apparatus and method for using multiple key codes with a single account number. This would allow, for example, for a family to set up a separate account for a wife's checking, for a wife's purchases, for a husband's purchases, and for the dependents' purchases. If desired, the same pin number could be used for all of these accounts. However, if, for example, the husband and wife wish the dependents from accessing excessive credit, they could limit the dependents' account to a specified maximum, and use a separate pin number for the children's account different from their own. Where multiple key codes are provided under one account number, the information sent to a merchant would remain the same as where there were only one key code. However, a particular key code would be sent to the bank, allowing the bank to account for the purchases under the different sub-accounts.

It is finally an object of the present invention to provide an apparatus and system which can be used with existing encryption technology such as SET, SSL, as well as with credit card set ups like the Nextcard®. The present invention simply adds additional security to such systems. In the case of the Nextcard the present invention would lessen the potential liability of the provider of the Nextcard.

There has thus been outlined, rather broadly, the more important features of the invention in order that the detailed description thereof that follows may be better understood, and in order

that the present contribution to the art may be better appreciated. There are, of course, additional features of the invention that will be described hereinafter and which will form the subject matter of the claims appended hereto.

In this respect, before explaining at least one embodiment of the invention in detail, it is
5 to be understood that the invention is not limited in this application to the details of construction and to the arrangements of the components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting. As
10 such, those skilled in the art will appreciate that the conception, upon which this disclosure is based, may readily be utilized as a basis for the designing of other structures, methods and systems for carrying out the several purposes of the present invention. Additional benefits and advantages of the present invention will become apparent in those skilled in the art to which the present invention relates from the subsequent description of the preferred embodiment and the
15 appended claims, taken in conjunction with the accompanying drawings. It is important, therefore, that the claims be regarded as including such equivalent constructions insofar as they do not depart from the spirit and scope of the present invention.

Further, the purpose of the foregoing abstract is to enable the U.S. Patent and Trademark Office and the public generally, and especially the scientist, engineers and practitioners in the
20 art who are not familiar with patent or legal terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The abstract is neither intended to define the invention of the application which is measured by the claims, nor is it intended to be limiting as to the scope of the invention in any way.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be better understood and the objects other than those set forth above will become apparent when consideration is given to the following detailed description thereof.

Such description makes reference to the annexed drawings wherein:

5 FIG. 1 is a schematic representation of the present invention.

 FIG. 2 is a flow chart illustrating the set up procedure.

 FIG. 3 is a flow chart illustrating the operation of the present invention.

 FIG. 4 is a symbolic representation of one system which can be used to implement the present invention, and particularly the sending of the various data packets.

10

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Referring now to the drawings, where like numerals represent like parts, the present invention incorporates an electronic apparatus 10 such as a personal computer. It should also be understood that, rather than using the personal computer, a net device such as a "web TV" system could also be used, though improvements and additional features may need to be made to web TV systems presently available before they could accommodate the present invention. In the future, additional devices (such as personal digital assistants) will be developed specifically to access the Internet and to perform transactions thereon. All of these devices can be represented by the electronic apparatus 10.

15 Cooperating with the electronic apparatus 10 is a display screen 12. The display screen 12 allows the electronic apparatus 10 to display various messages. Also cooperating with the electronic apparatus 10 are one or more data input devices 14. The data input devices 14 could be a keyboard, a mouse, a microphone for inputting the user's voice and/or voice commands, and

20

the like. Additional input devices are possible, and they are intended to be incorporated within the spirit of this invention.

Also incorporated within the electronic apparatus 10 is an article reader 18. It is anticipated that the article/media 16 will be, at least initially, a read-only compact disc. The article/media 16 could also be any number of other devices, such as a web card envisioned by U.S. Pat. No. 5,247,575. The card in question has the look of a typical credit card, but also can be read by a regular CD reader. A floppy disk with security features could also be used.

The electronic apparatus 10 will also have incorporated thereon a customer-specific software / code 20. There will, by necessity, need to be either memory or hard drive-type devices to store the customer-specific software / code 20. The electronic apparatus 10, also will preferably incorporate an electronic wallet 84. Electronic wallets are relatively new software elements. The electronic wallet 84 precludes the need for the user to specifically input his personal data, such as mailing address, social security number, and the like, when purchasing goods or services over the Internet. The electronic wallet 84 may also incorporate features to track expenditures on the Internet. The wallet will also facilitate use of multiple sub-account numbers, using different key code numbers under the same account number. The electronic apparatus 10 will also incorporate a communication means 21 for communication with a computer network 28. The communication means 21 may be a typical dial-up modem, a cable modem, a dedicated digital connection, a digital service line ("XDSL"), a satellite or other wireless connection, or the like.

Once a communication link is established via the communication means 21 with a computer network 28, a further link can be established with a supplier/merchant server or website 30. Goods and/or services may be offered for sale on the supplier/merchant server 30. The supplier/merchant server 30 may also be in communication with the merchant business server

34. This communication typically will occur through a firewall 32. Customers typically cannot contact the merchants business server 34 directly, because it is protected by the firewall 32. The merchants business server 34 further drives business processes 36. Business processes 36 include inventory control, shipping, and the like. The electronic apparatus 10 can also communicate via the computer network 28 with a bank Internet server 40. The bank Internet server 40 may also be in communication with multiple devices such as a download server 46, a purchase server 48, and a billing server 50, which are further in communication via a firewall 42 with the bank account information server 38. The bank account information server 38 is the bank's main computer where financial records and information on customers are kept. The bank account information server 38 may be in further communication through a bank network 52 with a merchant bank 80 or the customer's bank 86. The bank account information server 38 may also drive a media writer 44. The purpose of the media writer 44 is to create article/media to be sent to customers upon creation of a new account, modification of an existing account, or re-issue of an article for an existing account.

OPERATION

There are generally two phases to the operation of the present invention: first, a set up phase wherein the customer's or client's account is set up and codes are assigned, which is illustrated in FIG. 2; and second, an operation phase illustrated in FIGs. 3 and 4. FIG. 3 is a flow chart illustrating the operation of the present invention and FIG. 4 is a schematic representation of the flow of data among the bank, the customer, and the merchant.

FIG. 2 illustrates the set up phase. Set up starts when a customer contacts the bank or provider via a voice phone, Internet, e-mail, or regular mail. Additional means to set up an account may be available. It is not particularly relevant to the present invention whether the

account is set up over the phone, via the Internet, or via some other alternative method. However, it is preferable that the account be set up over the Internet to minimize paper work and costs. Upon contacting the bank, the customer supplies information regarding, for example, his name, mailing address, billing address (if different from his mailing address), e-mail address, and various other personal data required for the bank's purposes. Also at the time of application, the customer may select or be assigned a pin number to be used with his account. This pin number is either selected by the customer or assigned by the bank and communicated to the customer at or near the time the account is established. The customer has been made aware of his pin number by the time he has completed the application process. Making the customer aware of the pin number at the time the application is processed provides additional security. Since the pin is not supplied with subsequent setup information and equipment provided to the customer, someone wrongly intercepting a setup packet through the mail would not be able to use it because the pin number would not be included with the mailed information. Since the pin number will not be provided with the information mailed to the customer, it is preferable that a reminder electronic communication be sent to the customer at the time the account is established, the communication verifying acceptance of the customer's application and noting the customer's pin number.

A customer may also request multiple sub-accounts under the same account number. These sub-accounts may be, for example, for separate accounts for a husband and wife. Separate accounts could also be provided for dependent children. Each of these accounts could have separate provisions for credit limits. They could all use the same pin number, or they could have different pin numbers for each account or for groups of accounts. These separate sub-accounts would be particularly useful for institutional climates, such as cities or corporations. The entity could set up a master account, then give sub-account numbers to each department or division with separate credit limits and pin numbers. One billing statement would then be provided to

the entity summarizing the purchases made under the sub-accounts. Each department or subdivision of the entity could be given a separate version of the article 16 for its account. A method is disclosed using multiple accounts. The method of multiple accounts is set up by a method of providing the electronic apparatus 10, creating a customer account at a bank pursuant to communication with the customer; creating customer-specific software 20 at the bank, then splitting the software 20 into a first portion 22, which is written to an article 16, and a second portion 24 which is transmitted to a bank download server 46; providing more than one key code number, each corresponding to a sub-account depending from the same account number; mailing the article 16 to the customer who then inserts it into his electronic apparatus 10; the customer contacting the bank download server 46 via the Internet and downloading the second portion 24 to the electronic apparatus 10, then the bank download server 46 erasing the copy of the second portion 24 from the download server, but retaining relevant information on the bank purchase server 48; and the electronic apparatus 10 linking the first 22 and second 24 portions into working software 20; and the bank accounting separately for purchases under each key code number. As noted, one variation of this method is the creation of multiple articles 16 for the same account where multiple departments or sub-divisions are planning to use the same account. With multiple copies of the article 16 there is no need for a user to search for the common article each time a purchase is to be made.

Once the application is complete, the bank performs a credit check. If the customer is approved, the bank server 38 generates a unique version of the operating software 20 (which may also be referred to as "operational code") and associated account numbers for the customer (i.e., an account number, pin number, and key code number). If the customer's application is rejected, such rejection is communicated to the customer.

Assuming the application is approved, the unique software 20 is then split into two portions, a first portion 22, and a second portion 24. The bank media server 44 writes the first portion 22 to the article/media 16. The article/media 16 is then mailed to the customer. The customer inserts the article/media 16 into his electronic apparatus 10. Some portion of the first portion 22 may then be written to a storage medium (such as a hard drive) on the electronic apparatus 10. This splitting of the operational software / code 20 is a security feature; the system cannot be used with the first portion 22 alone. Further, the second portion 24 cannot be obtained without the pin number, which would be unknown to someone who improperly intercepted the article / media 16.

At or near the same time as the first portion 22 is written to the article/media 16, the second portion 24 is transferred from the bank server 38 to a download server 46. The second portion 24 remains on the download server 46 for a specified time period. If the customer does not connect to the download server 46 within a specified time, the second portion 24 is erased from the download server 46. However, if the customer connects to the download server 46 within the specified time, the download server 46 performs a checksum. The user must enter his pin number 68, which is required to allow him to download the second portion 24, the necessary code is then written to a storage device (e.g., either a hard drive or RAM). If the checksum is not acceptable, an error message is displayed, and the customer is instructed to either contact the bank or a service provider to further explore what has happened to prevent him from successfully downloading the second portion 24. The customer must have inserted the article / media 16 into his electronic apparatus 10 and, pursuant to the programming, some portion of the software / code may have been written to the storage medium to satisfy the checksum. Further, the customer will be prompted to enter his pin number. If the checksum is successful, the second portion 24 is downloaded to the customer's electronic apparatus 10.

The first portion 22 and the second portion 24 are then linked in the users's electronic apparatus 10 to form operational software / code 20. Linking is not equivalent to re-compiling the first and second portion 22 and 24. Rather, linking amounts to recording appropriate information regarding the electronic apparatus 10 (such as IRQ addresses), the intercommunication of the two portions, and other pertinent information into appropriate code lines on the portion stored on the electronic apparatus 10. Thus, neither piece of the puzzle, the article / media 16 nor the portion of the operational code 20 stored on the electronic apparatus 10 alone is sufficient to operate the system. Both must be present for the system to function. The operational code / software 20 is formed by the two linked portions both being present in the electronic apparatus 10 at the same time. The pin number must be entered before the linking will be accomplished.

Once linking has been successfully completed a display 12 displays a message indicating that the present invention is ready for operation. At or near the same time, the second portion 24 is deleted from the download server 46. Thus, the software has been successfully set up on the user's electronic apparatus 10. The bank purchase server 48 maintains a copy of the needed information regarding the user. After the second portion is deleted from the download server 46, the software cannot be installed on another machine without re-contacting the bank to have the second portion again sent to the download server 46.

As with account setup for customers, accounts for merchants can be created via communication on the telephone, regular mail, e-mail or by other communication means. Once a merchant account is established, the merchant downloads a serialized copy of the merchant transaction software from the download server 46. The merchant transaction software incorporates a detection routine, which determines the nature of the merchant's application programming interface ("API"), then installs appropriate code within the merchant's web server

application. The merchant's web server application does not need to be re-programmed from scratch. Rather, a "patch" is installed to add a branded payment button for the present invention, which, when selected by the customer, triggers the operation of the present invention.

FIG. 3 illustrates the operation of the system, once the system has been set up. The user first connects to a merchant server 30. This connection is established to or through a computer network 28 such as the Internet. The user or customer then selects the goods or services to be purchased. The customer then selects the present invention as the method of payment. At that time, the operational code / software 20 performs a checksum to ensure the article 16 is in place. If the article 16 is not in place, the customer is prompted to install it. No transactions will be allowed using the present invention until the article 16 is installed. Once the article is installed, the customer is prompted to enter his pin number. The software then transmits the order, a first part of which — the order packet 56 — is sent to the merchant with a second part — the bank packet 58 — sent to the bank 48. Upon receipt of the bank packet 58, the bank purchase server 48 begins scanning incoming data for a merchant packet 60 corresponding to the bank packet 58. Common data 66 contained in both the merchant packet 60 and the bank packet 58 enable the two to be matched by the bank purchase server 48. If the two packets arrive at the bank purchase server 48 within a specified time frame, a checksum is performed to verify that the account number 74, the pin number 68, as well as the keycode 72 match, and finally that the merchant number 76 is valid. If, however, too much time has elapsed between the time the bank packet 58 arrives at the bank purchase server 48 and the time the merchant packet 60 arrives, a message is displayed that too much time has elapsed, please place the order again, or similar message. When the checksum is performed, if it is successful, the bank purchase server 48 generates an approval packet 62. If the checksum is unsuccessful, a message is relayed to the electronic apparatus 10 of the user and the merchant, indicating that there was a problem with your order;

please try again or call the bank, or similar message. Upon approval, an approval packet 62 is then transmitted to the merchant 30. The merchant generates a confirmation packet 64, which is transmitted to the user's electronic apparatus 10. At the same time, the merchant server 30 sends a command to the merchant business server 34 to deliver the goods or services. The
5 business processes 36 within the merchant's organization complete this operation. In a preferred embodiment, simultaneously with the transmission of the approval packet 62 to the merchant, a payment 88 is transferred to the merchant bank 80 via bank networking 52.

FIG. 4 illustrates one system of transmitting data among the bank purchase server 48, the customer's electronic apparatus 10, and the merchant web server 30. The data packets corresponding to the system shown in FIG. 4 are shown below:

| Order Packet — 1A (56) | | Bank Packet — 1B (58) | |
|--------------------------|--------------------------------------|--------------------------|------------------------|
| 1. | Purchase No. | 1. | Purchase No. |
| 2. | Dollar Amount | 2. | Dollar Amount |
| 3. | Name | 3. | Keycode (72) |
| 4. | Address (shipping) | 4. | Pin No. (68) |
| 5. | Description of goods / services (70) | | |
| 6. | Account No. (74) | | |
| Merchant Packet — 2 (60) | | Approval Packet — 3 (62) | |
| 1. | Purchase No. | 1. | Purchase No. |
| 2. | Dollar Amount | 2. | Dollar Amount |
| 3. | Account No. (74) | 3. | Authorization No. (78) |
| 4. | Merchant No. (76) | | |

The process is initiated by an order packet 56 and a bank packet 58 being sent by the customer's electronic apparatus 10. The order packet 56 comprises, at least:

- common data 66 (i.e., a purchase number and a dollar amount); and
- the customer's name and address, which are automatically sent to the merchant pursuant to information provided the bank at the time the account is set up;
- the customer's account number; and
- a description of the goods and services to be purchased 70.

The customer may indicate that he wishes to have the goods or services shipped to an alternative address, in which case he will check a box on the order form. The alternative address will then be provided by the customer, and this will be the address to which the goods are shipped, rather than the address provided to the bank at the time the account was set up. The purchase number is generated by the software 20 installed on the electronic apparatus 10. A log, preferably sorted by purchase order number, is maintained both on the electronic apparatus 10 and at the bank purchase server 48 detailing charges made by the customer.

Both the bank packet 58 and the order packet 56 contain common data 66. The common data 66 is the purchase number and the dollar amount. Also sent in the bank packet 58 is a keycode 72 indicating whether or not the article 16 is present in the article reader 18. Finally, included in the bank packet 58, is the pin number 68.

Upon receipt of the order packet 56 the merchant 30 generates a merchant packet 60. The merchant packet 60 includes the common information 66 (namely the purchase number and dollar amount) as well as the account number 74 and a merchant number 76. The merchant number 76 is provided to the merchant upon establishing a merchant account with the bank. The merchant packet 60 is then sent to the bank purchase server 48 via the computer network 28.

Upon receipt of the merchant packet 60, the bank purchase server 48 attempts to match the merchant packet 60 with the bank packet 58. This matching occurs via the common information 66. If a match is made, the bank attempts to determine whether sufficient credit remains to authorize the purchase. If sufficient credit remains, an authorization number 78 is generated. This type of authorization approval is commonly performed with existing systems for purchasing goods and services over the Internet. The nature of the bank's internal approval process is not a critical part of the present invention. The common information 66 and the authorization number 78 are prepared into an approval packet, which is relayed back to the

merchant. After receiving the approval packet 62, the merchant sends a confirmation packet 64 of the sale back to the user's electronic apparatus 10. The confirmation packet 64 is typically generated in transactions occurring today on the Internet, and the specific contents of this packet are not particularly relevant to the present invention. However, it is preferable that the confirmation packet 64 includes at least the purchase number, the dollar amount of the purchase, and a description of the goods and services purchased by the customer. The confirmation packet 64 may also include the merchant's name as well as the date / time of the purchase and the shipping address used.

Billing may be accomplished by standard mail, as with traditional credit cards. Alternatively, an on-line billing system used in conjunction with the Internet only credit card whereby billing statements, instead of being sent by regular mail, are sent by e-mail to the customer. This takes advantage of the fact that e-mail is free, incurring no mailing charges for the credit card issuer. In addition, billing transactions are more rapidly completed as are payment transactions. In fact, using the present invention, there could be transactions that are completely paperless. That is, transactions where no paper is sent from or to any of the parties involved in the transaction. Once a customer receives an e-mail bill, he can merely check a payment method on the e-mail, then press a respond key in the e-mail to forward payment. The e-mail bill may offer the customer a variety of payment methods (e.g., bank draft, or paper check sent under separate cover). At the time the customer's account is established, the customer may choose a preferred method of payment for electronic billing.

Having thus described the invention, I claim:

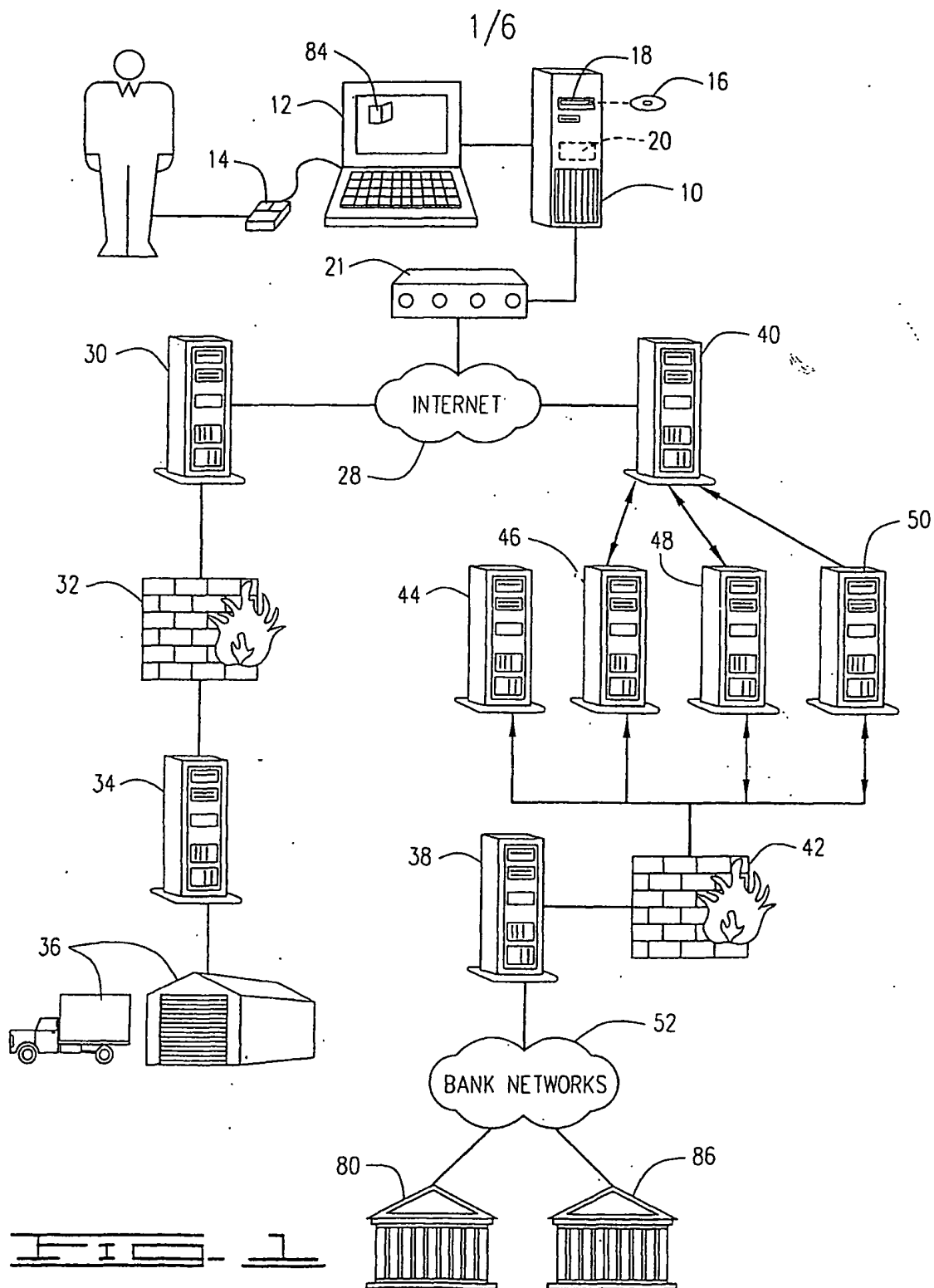
1. An electronic apparatus for providing security of specified electronic transactions, the electronic apparatus comprising:
 - a. an article removably inserted into the electronic apparatus, the article bearing machine readable code;
 - 5 b. customer-specific code installed on the electronic apparatus, the code affecting operation of the electronic apparatus;
 - c. verifying means for determining whether the article is installed in the electronic apparatus, and, if so, for enabling specified electronic transactions, but, if not, for preventing said transactions;
- 10 whereby, upon a specified request by the user, the electronic apparatus queries whether the article is installed, and, if so, enables specified transactions to be performed at the request of the user, but prevents the transaction from being performed if the article is not installed.

2. A purchasing method of purchasing goods and services via the Internet comprising the steps of:
- a. a customer accessing a merchant's server and selecting desired goods and services and placing an order for same, the order resulting in the transmission of an order packet to the merchant and a bank packet to a bank's purchase server;
 - b. upon receipt of the order packet, the merchant generating a merchant packet and transmitting same so that it is received by the bank's purchase server;
 - c. the bank's purchase server matching the merchant packet with the bank packet using the common information as a key;
 - d. the bank's purchase server checking for accuracy of both the merchant and bank packet and determining whether sufficient credit remains on customer's account to authorize the transaction;
 - e. approving the transaction if step d is satisfactory, and transmitting an approval packet so that is received by the merchant.

3. A setup method for setting up a system to implement the method of purchasing goods and services via the Internet, the setup method comprising the steps of:
- a. providing the electronic apparatus of claim 1;
 - b. creating a customer account at a bank pursuant to communication with the
5 customer;
 - c. creating customer-specific software at the bank, then splitting the software into a first portion, which is written to the article and a second portion which is transmitted to a bank download server;
 - d. mailing the article to the customer, who then inserts it into the electronic
0 apparatus;
 - e. the customer contacting the bank download server via the Internet and downloading the second portion to the electronic apparatus, then the bank download server erasing the copy of the second portion from the download server, but retaining relevant information on a bank purchase server; and
 - f. the electronic apparatus linking the first and second portions into working
5 software on the electronic apparatus.

4. A billing method for billing customers for purchases made using the purchasing method of claim 2, the billing method comprising the steps of:
- 5
- a. upon completion of a transaction or a set of transactions, the bank sending an electronic communication via the Internet to the customer listing the purchase made and the total amount due;
 - b. the customer selecting a method of payment and responding with same in an electronic communication via the Internet back to the bank; and
 - c. the bank completing the payment pursuant to instructions from the customer in the response electronic communication.

5. The method of claim 3, additionally comprising the steps of:
- a. in step b of claim 3, providing more than one key code number, each key code corresponding to a sub-account depending from the same main account;
 - b. providing additional steps in the code which require a customer to select the key code that is to be used for a specific purchase, then providing for that key code to be sent to the bank purchase server along with the bank packet; and
 - c. accounting separately for the purchases made by a customer under each separate key code number.



2/6

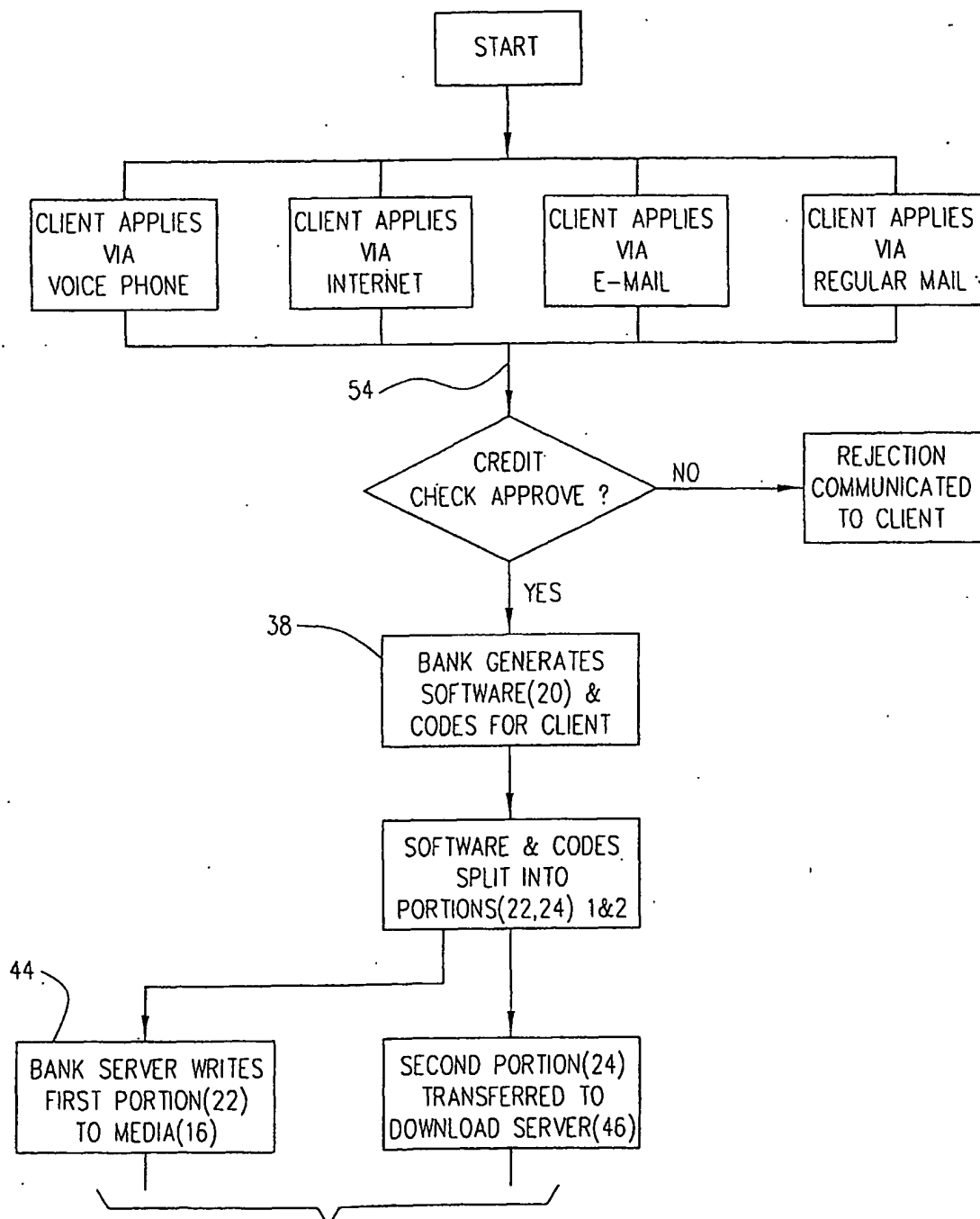
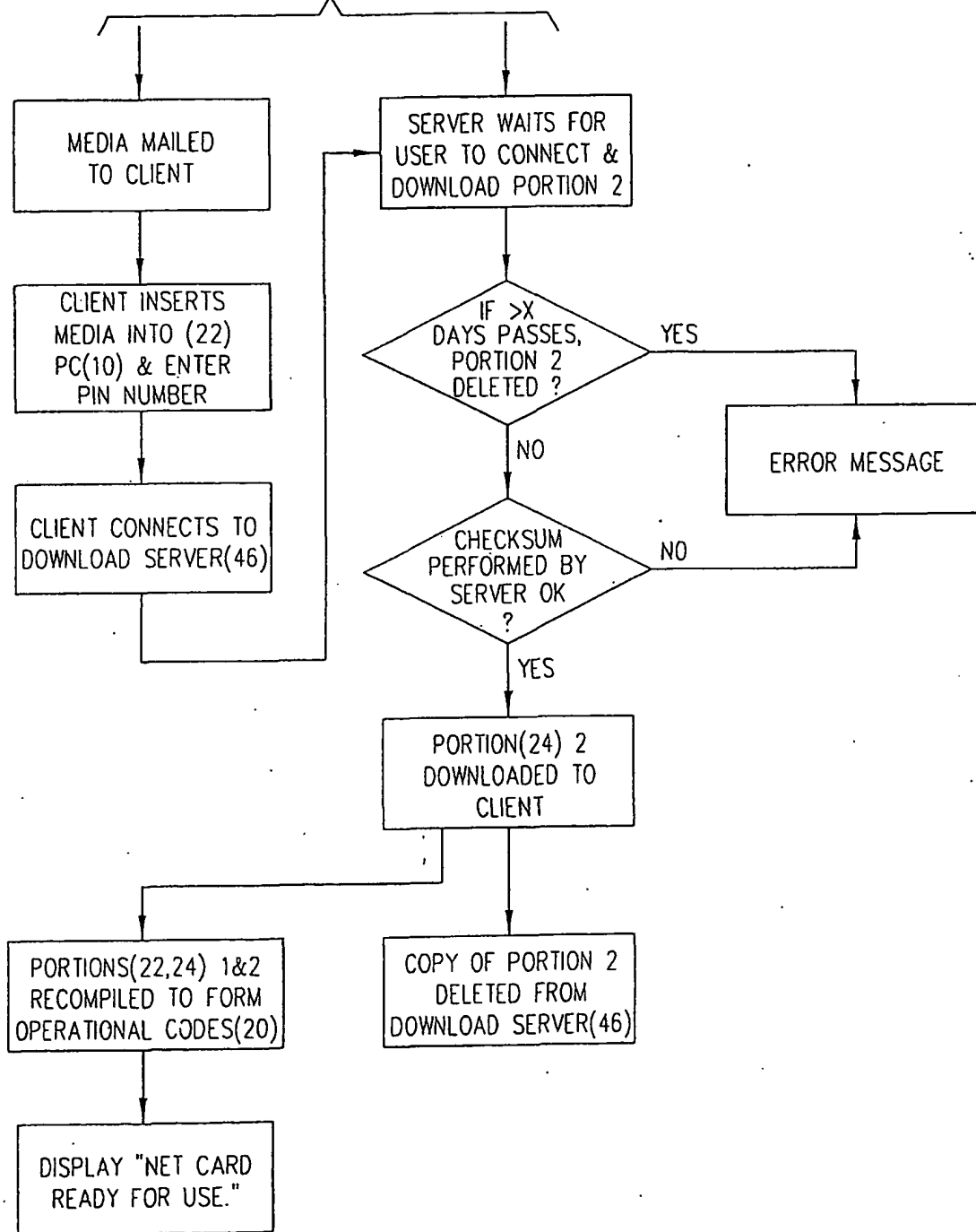


FIG. 2B

FIG. 2A

3/6

FIG. 2A

FIG. 2A

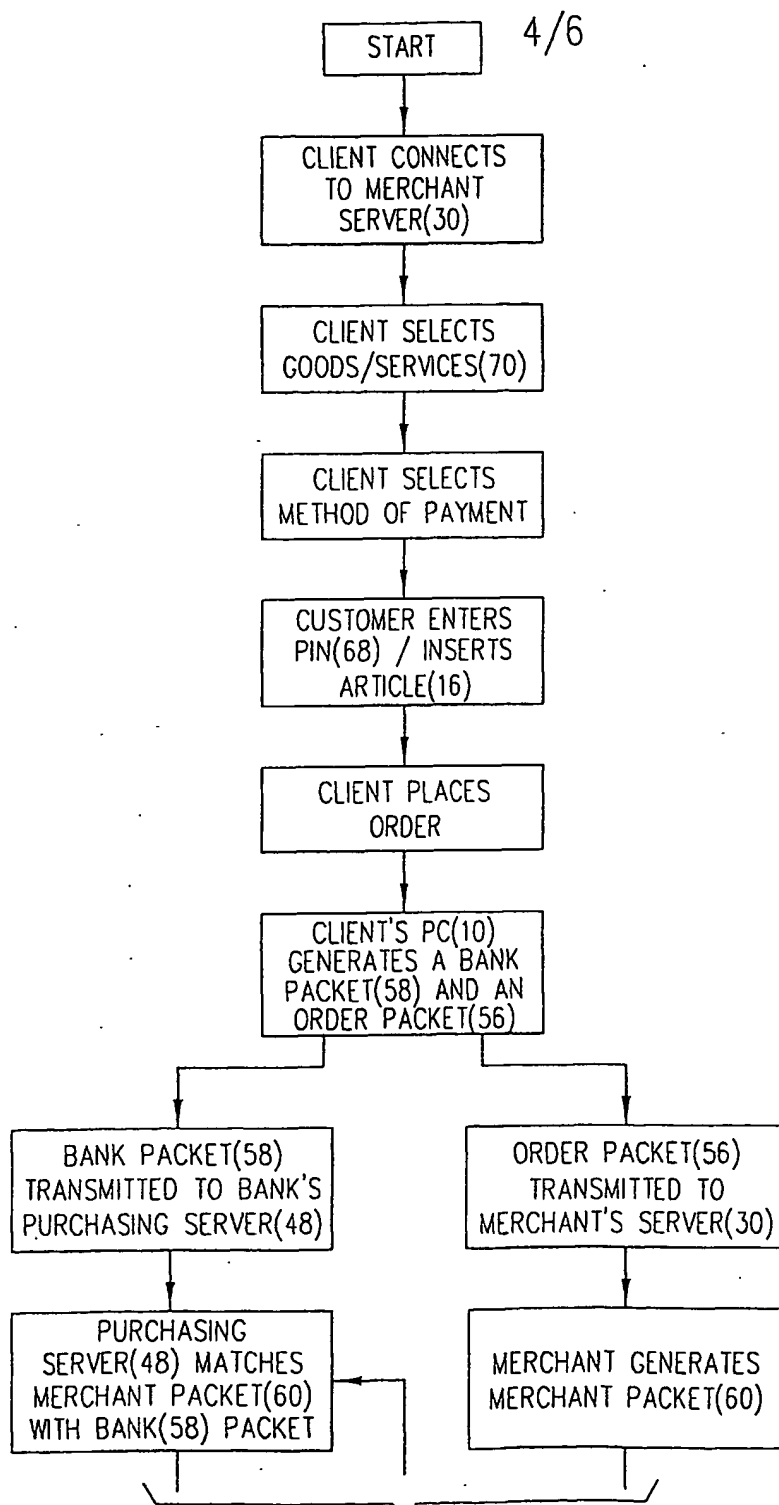
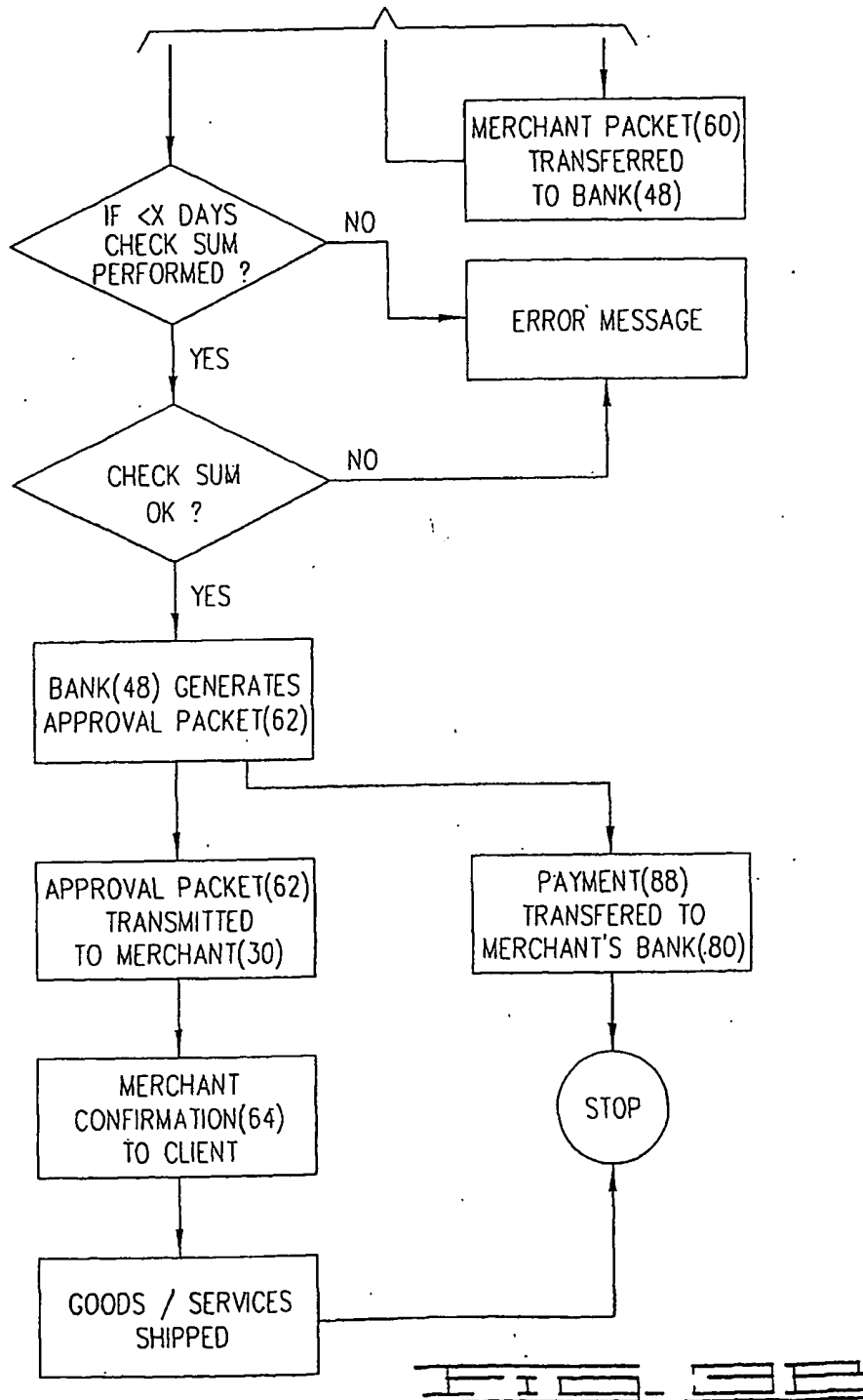


FIG. 3B

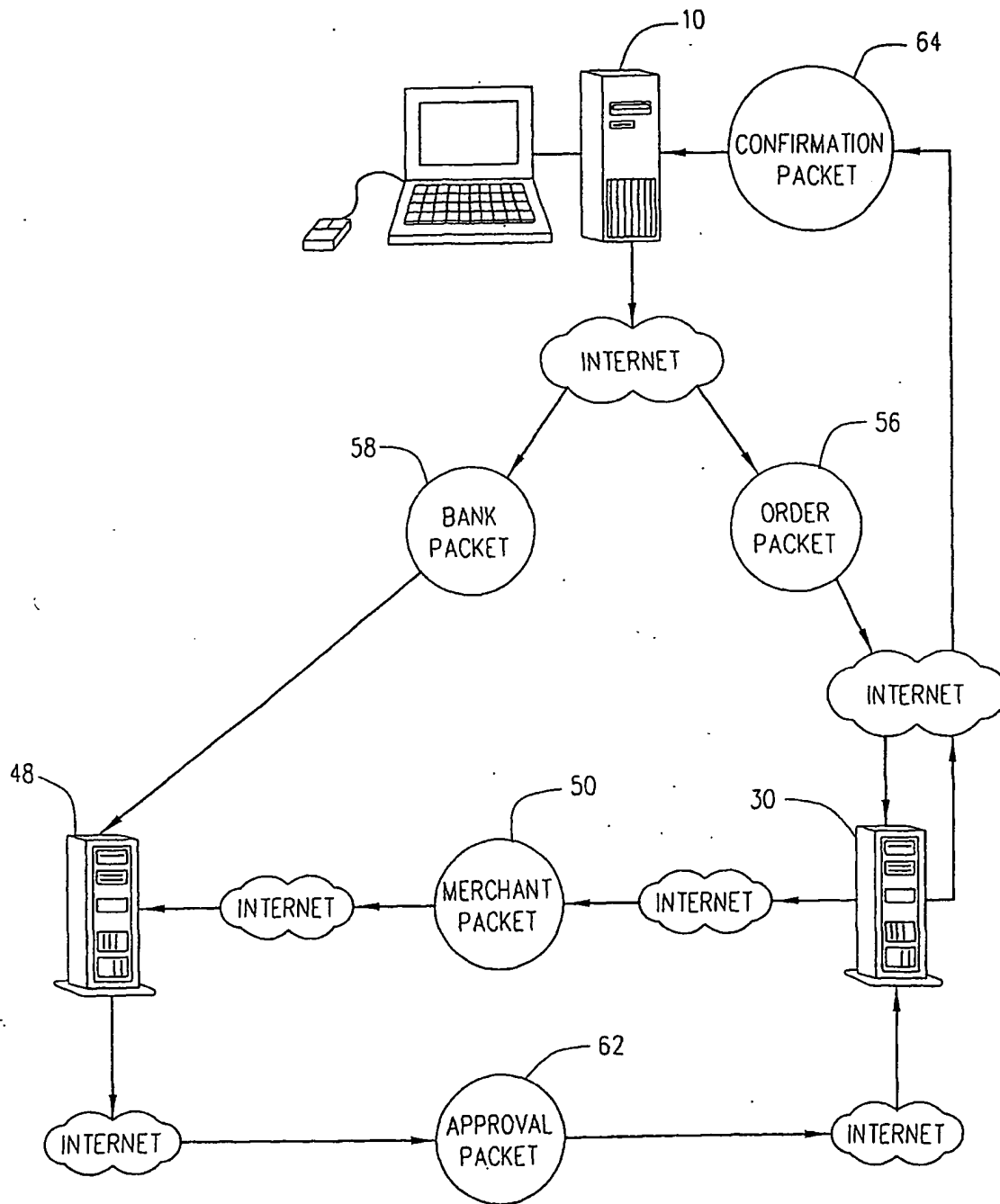
FIG. 3A

5/6

FIG. 3A



6/6

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/22373

| A. CLASSIFICATION OF SUBJECT MATTER | | |
|---|--|-----------------------|
| IPC(7) : Please See Extra Sheet. | | |
| US CL : 705/26, 27, 44, 65; 713/200; 369/272; 235/380; 221/12 | | |
| According to International Patent Classification (IPC) or to both national classification and IPC | | |
| B. FIELDS SEARCHED | | |
| Minimum documentation searched (classification system followed by classification symbols) | | |
| U.S. : 705/26, 27, 40, 41, 44, 65; 713/155, 200, 201; 369/272; 235/380; 221/12; 716/11 | | |
| Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched | | |
| Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) | | |
| PROQUEST, DIALOG | | |
| Search Terms: Purchasing/Ordering Method, Split Key, Dongle, Computer Security | | |
| C. DOCUMENTS CONSIDERED TO BE RELEVANT | | |
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| X — Y | US 3,651,986 A (KARECKI et al.) 28 March 1972, col. 3, lines 28-36; col. 3, lines 11-16; col. 4, lines 44-53. | 1 — 3, 5 |
| X — Y | US 5,590,197 A (CHEN et al.) 31 December 1996, col. 5, lines 1-5; col. 5, lines 29-40; col. 6, lines 27-31; col. 6, lines 12-31. | 1 — 3, 5 |
| A | US 4,562,306 A (CHOU et al.) 31 December 1985, col. 5, lines 21-23; col. 4, lines 24-31. | 1, 3, 5 |
| A | US 5,826,241 A (STEIN et al.) 20 October 1998, col. 6, lines 17-23. | 2-5 |
| A | US 5,903,878 A (TALATI et al.) 11 May 1999, col. 6, line 44. | 2-5 |
| <input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex. | | |
| * Special categories of cited documents: | *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art *Z* document member of the same patent family | |
| *A* document defining the general state of the art which is not considered to be of particular relevance | | |
| *B* earlier document published on or after the international filing date | | |
| *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | | |
| *O* document referring to an oral disclosure, use, exhibition or other means | | |
| *P* document published prior to the international filing date but later than the priority date claimed | | |
| Date of the actual completion of the international search | Date of mailing of the international search report | |
| 23 OCTOBER 2000 | 12 JAN 2001 | |
| Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 | Authorized officer TARIQ HAFIZ | |
| Facsimile No. (703) 305-1936 | Telephone No. (703) 308-7808 | |

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/22373

| C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT | | |
|---|---|-----------------------|
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| A | US 5,889,941 A (TUSHDIE, et al.) 30 March 1999, col. 3, lines 1-8. | 1-5 |
| A, P | "Wave Systems' E-Commerce Bundled with Kiss Nordic Multimedia," Multimedia Publisher. 01 October 1999, p. 1. | 1-5 |
| A | TYLER, GEOFF., "The Card from Nowhere," Management Services. February 1996, p. 28. | 1-5 |
| A | REISMAN, RICHARD R. "CD-ROM/Online Hybrids: The Missing Link?" CD-ROM Professional. April 1995, pp. 1-9. | 1-5 |
| A | US 5,036,461 A (ELLIOTT et al.) 30 July 1991, col. 9, lines 56-68; col. 10 lines 1-9. | 1, 3, 5 |
| A | US 4,968,873 A (DETHLOFF et al.) 06 November 1990, col. 5, lines 54-64. | 1, 5 |
| X | US 5,513,169 A (FITE et al.) 30 April 1996, col. 1, lines 63-67. | 1 |
| Y, E | US 6,108,420 A (LAROSE et al.) 22 August 2000, col. 3, lines 27-57. | 1 |
| Y | US 5,341,429 A (STRINGER et al.) 23 August 1994, col. 3, line 64; col. 4, line 1; col. 5, line 34; col. 7, line 34. | 2-5 |
| Y | US 5,892,825 A (MAGES, et al.) 06 April 1999, col. 3, line 62. | 2-5 |
| Y, P | US 6,032,134 A (WEISSMAN) 29 February 2000, col. 2, line 25; col. 5, line 17. | 5 |
| Y | US 5,495,411 A (ANANDA) 27 February 1996, col. 2, line 51; col. 3, line 16. | 2-5 |
| Y | US 5,692,049 A (JOHNSON et al.) 25 November 1997, col. 4, line 52; col. 5, line 15. | 2-5 |
| Y | US 5,864,830 A (ARMETTA, et al.) 26 January 1999, col. 4, line 4. | 5 |

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/22373

Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/22373

A. CLASSIFICATION OF SUBJECT MATTER:

IPC (7):

G06F 17/60, 11/30, 12/14; H04L 9/00, 9/32; G11B 3/70, 5/84, 7/26; G06K 5/00; G07F 11/00

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING

This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claims 1, 3, and 5, drawn to an electronic apparatus and method for providing security.

Group II, claims 2 and 4, drawn to a purchasing and billing method.

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claims 1, 3, and 5, drawn to an electronic apparatus and method for providing security.

Group II, claims 2 and 4, drawn to a purchasing and billing method.

The inventions listed as Groups I and II do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

Invention II comprises a purchasing and billing method and has separate utility in use with any generic security apparatus. The use of various and different security apparatus configurations is accomplished through the use of passwords, digital signatures, hardware attachments to computers, transportable media such as floppy disks and magnetic tapes, and separate and distinct software files

Invention I comprises an electronic hardware apparatus for providing security and has disparate technical features from Invention II. These inventions have acquired a separate status in the art and are shown by different classifications.